국내외 CMVP 정책 동향에 관한 연구

최명길*, 정재훈**,
*중앙대학교 사회과학대학
**중앙대학교 경영대학
e-mail : selpine@naver.com

A study on domestic and foreign policy trends of CMVP

Myeong-Gil Choi*, Jae-Hun Jeong**
*College of Social Sciences, Chung-Ang University
**College of Business Adminstration, Chung-Ang University

요 약

정보통신분야의 발전으로 인해 익명성의 사이버 사회가 도달하였고 해킹과 같은 역기능이 많이 발생함에 따라 정보보호를 위해 암호모듈에 대한 수요가 급증하고 있다. 하지만 국내에서는 암호모듈에 대한 평가 기준 정립이 미흡하여 수요자가 모듈 선택 시 어려움이 있고, 모듈 및 제품 상호간의 운용 및 호환성 확보에 어려움이 있다.

본 논문은 정보보호 제품에 대한 안전성을 평가해 제품의 신뢰성을 높이고, 기술의 향상을 유도하는 국외의 정보보호 제품에 대한 평가 프로그램인 CMVP의 현황을 살펴본다. 이를 통해 다가오는 국제표준에 대비하여, 국내 정보보호 제품 보호와 기술보호를 위해 선진외국의 제도, 기술, 현황분석 및 국제 암호제도 공조체계 구축을 위한 기반을 제공코자 한다.

1. 서론

암호 기술의 표준화로 인하여 정보 보호 업체들은 표준화된 암호 기술을 채택하여 안전하고 신뢰성 있는 제품을 생산할 수 있게 되었다. 그러나 이러한 암호 기술의 이해 부족 및 실제 구현상의 미스 등으로 인해 실제 제품에 탑재하는데 완전성을 보장하는데 불충분하는 경우가 발생하기도 한다.

특히 우리 나라는 정보보호제품에 대한 평가는 활발하지만, 암호모듈 평가는 미국 등의 선진국과 비교하였을 때 완전히 정착되지 않아 선진국 수준의 제도 및 절차의 정착이 시급하다. 따라서 글로벌 수준의 암호모듈 평가 및 검증 절차를 확립을 위하여 국외 암호모듈 정책, 제도, 법 등의 연구 동향 및 정책을 연구할 필요가 있다.

정보보호 기능은 모든 유형의 '정보시스템'의 기본 기능이다. 정보시스템이 정보보호 기능 중 기밀성, 무결성 등의 보안 서비스를 제공하기 위해 '암호모듈'을 상요한다. 암호모듈은 보안 서비스를 제공하기 위한 보안 프로토콜, 보안 메커니즘 및 암호 알고리즘이며 하드웨어, 소프트웨어 또는 펌웨어로 구현된다.

최근의 이러한 암호기술의 안전성 평가는 가장 기본이 되는 안전성 요구이므로 국내외적으로 암호알고리즘의 안전성 분석 및 암호모듈의 안전성 평가에 대해 많은 관심을 보이고 있으며, 특히 미국에서 암호모듈의 '시험과 검증'(test & verification)은 CMVP를 통해 실시한다. CMVP는 미국과 캐나다에서 운영 중인 암호검증체계이며 NIST의 FIPS 140-1, FIPS 140-2를 거쳐 새로운 기준인 FIPS 140-3 기준과 구체적인 시험기준인 DTR(Derived Test Requirement)을 기반으로 한다.

미국의 CMVP는 우리나라와 일본의 암호 모듈검증체계의 모델이다. 향후 CCRA처럼 'CMVP 상호인정(CMVP RA) 제도'가 실시될 것으로 예상된다.

본 논문은 국외의 암호 모듈 평가 프로그램인 CMVP에 대하여 선진각국의 제도, 기술 동향을 분석하고 검증된 제품 분석을 통하여 정책과 방향을 정립하여 국내에서 진행 중인 KCMVP의 국제 표준화로의 체계 구축을 위한 환경과 기술개발의 기반제공에 기여코자 한다.

2. 국내외 암호모듈 정책 현황

암호화모듈 검증제도는 암호 기능이 들어간 정보보

호 제품을 공공기관에 공급할 때, 반드시 검증필을 받은 암호화모듈을 사용해야 하는 제도를 말한다.

정보시스템은 정보보호를 위해 암호모듈을 사용한다. 그러나 단순히 표준화된 암호모듈의 사용 및 배포는 충분한 수준의 정보보호서비스를 제공할 수 없다. 암호모듈의 운영자가 모듈이 제공하는 보안이나 기능을 충분히 숙지하고, 암호모듈 사용자에게 암호모듈 사용시 발생할 수 있는 잔여 위험을 공지해야 한다.

2.1. 미국 및 캐나다의 암호모듈 검증제도 분석

미국은 CMVP(Cryptographic Module Verification Program)를 통해 암호모듈을 '시험 및 검증'(test & verification)한다. FIPS 140 시리즈는 사실상의 국제표준이며, 실제 암호모듈 검증을 위한 국제기준인 ISO/IEC 19790은 FIPS 140-2와 거의 동일하다. ISO/IEC 24759는 ISO/IEC 19790을 위한 시험기준인 DTR에 해당한다.

▪ FIPS 140-1(1994년)은 개발자에게 융통성을 부여하고 하드웨어 중심이며, 소프트웨어로 구현된 암호모듈도 암호모듈로 간주하기 시작하였다.

▪ FIPS 140-2(2001년)는 FIPS 140-1을 재구성하고 요구사항을 명확히 하였으며, 개발자가 검증자를 위한 DTR을 개발하였고 설계보증개념을 추가하였다. ISO/IEC 19790 (2006년)은 FIPS 140-2를 국제 표준화한 것이며 내용을 일부 변경하였다.

▪ FIPS 140-3은 2007년 7월에 초안이 발표되었고, 2009년 11월에 개정 초안이 발표되었다. FIPS 140-3은 최신의 고급 보안 기술 및 방법을 반영하기 위해 기존의 문서에 새로운 보안 기능을 추가하였다. 새로운 소프트웨어 및 펌웨어 보안 영역과 보호되지 않는 요구사항을 포함한 비침투공격을 고려하여 소프트웨어 및 펌웨어 요구 사항을 지정하였다.

DTR은 FIPS 140-2를 기준으로 시험 및 검증시 각 보안요구사항 영역(area)별로 '시험항목' 및 '시험절차'를 상세히 명세한 문서이다. NIST의 CMVP 체계에서는 DTR에 따른 시험지침을 별도의 '구현지침'으로 발표하고 있다.

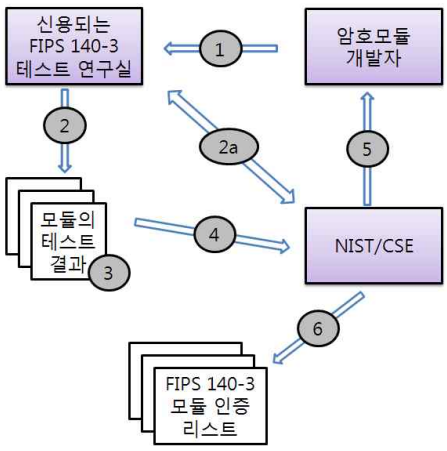
FIPS 140-3은 보안등급을 4단계로 나누고 있다. 본래 FIPS 140-3 초안에는 5단계로 나누고 있으나, 기존의 보안등급과 정확히 대응되지 않아 4단계로 구분한다. [표 1]은 보안등급을 나타낸 것으로, FIPS 140-3의 각 요구사항영역에 해당하는 보안등급 내역을 나타내고 있다.

[표 1] FIPS 140-3의 보안등급

보안등급 / 요구사항 영역	보안등급 1	보안등급 2	보안등급 3	보안등급 4
1. 암호모듈 명세	- 모듈, 범위, 승인된 알고리즘 및 승인된 동작모드의 명세 - 모듈 HW/SW의 기술 - 모듈의 문서화			
	- 보안정책은 승인된 동작모드		- 모듈의 승인된 동작모드를 표시	
2. 암호모듈 포트 및 인터페이스	- 요구된 선택적 인터페이스 - 모든 인터페이스 및 모든 입력 및 출력 자료경로의 명세		- 다른 포트와 인터페이스로부터 안전한 채널을 사용한 CSP 입력 및 출력	
3. 역할, 서비스 및 인증	- 모듈의 역할 및 서비스의 정의	- 역할기반 또는 신분 기반 인증	- 신분기반 관리자 인증	- Multi-factor 인증
4. S/W 보안	- 실행가능 코드, 승인된 무결성 기법	-전자서명 기반 무결성 시험	- S/W 무결성 시험	- CSP 및 무결성 시험 코드의 암호/복호화
5. 운영환경	-단일사용자 OS 또는 재량적 접근통제	- 감사 메커니즘	- 암호 SW, SSP 및 자료 보호	- 확장형 감사 요구사항
6. 물리적 보안	- 제품수준 컴포넌트	- 불투명 덮개나 외장	- 탈착식 덮개 및 문에 불법조작 대응 및 차단 회로	- 온도 및 전압을 위한 EEP

CMVP에서 진행되는 평가는 FIPS 140시리즈의 DTR 문서에 의해 진행된다. CMVP에 따른 모든 시험은 CMTL(Cryptographic Module Testing Laboratory)로 인정된 제3자 시험기관에서 수행된다.

CMVP의 평가 절차는 [그림 1]와 같다.



[그림 1] CMVP 평가 절차

2.2. 영국의 암호모듈 검증제도 분석

영국의 정보보증업무를 총괄하는 CESG (Communication and Electronics Security Group)는 상용 암호모듈을 탑재한 암호제품의 정부 조달을 지원하기 위해 CAPS (Cryptographic Assisted Products Scheme)를 시행하고 있다.

CAPS는 국가기관에서 사용되는 암호제품을 3단계의 보안등급(Baseline, Enhanced, High)으로 구분하고 있으며, 비밀로 분류되지 않은 데이터보호를 목적으로 암호제품에 탑재된 암호모듈 및 암호알고리즘의 경우 CMVP를 통해 검증된 것의 사용을 권고한다. 현재 영국에는 2개의 CMTL이 존재하며, 10개의 검증완료 암호모듈이 존재한다.

2.3. 일본의 암호모듈 검증제도 분석

일본 정부는 비밀로 분류되지 않은 데이터 보호를 위해서 사용되는 암호모듈 및 암호알고리즘을 국가기관의 사용을 위해서 JCMVP(Japan CMVP)를 운영한다. JCMVP는 북미 CMVP와 동일한 암호모듈 보안요구사항 및 시험기준을 채택하고 있다. 2006년 6월 시험운용을 통해 2007년 4월부터 정식 시행 중이다. 최근 미국과 상호협력체계를 구축하여 각 지역의 시험기관에서 시험한 제품에 대해 미국과 일본 기관은 상호 인증하고 있다.

2.4. 국내의 암호모듈 검증제도 분석

국가정보원은 정보화촉진기본법 및 전자정부법 등 관련 법규에 의거, 정보보호제품 평가·인증제도 운영 및 국가기관에 도입되는 상용 정보보호제품의 보안적합성 검증 서비스를 총괄한다. 이중에서 국가기관이 사용하는 상용 암호모듈의 시험 및 검증 등에 필요한 사항은 “암호모듈 시험 및 검증지침”(행자부 고시, 제2004-45호)에 규정하고 있다.

국가정보원은 검증된 암호모듈을 탑재한 정보보호제품의 국가기관 도입을 지원하기 위해 보안적합성 검증제도를 시행하고 있고, 이러한 제품이 암호논리의 안전성, 구현 적합성, 공격에 대한 내구성 측면에서 국가기관에서 사용이 가능한지의 여부를 결정하기 위해 비공개 기준을 적용한다.

2.5. 각국의 암호모듈 검증기준

대부분의 국가가 암호모듈 검증절차로 CMVP를 사용하고 있으며, 현재 가장 활성화된 암호모듈 검증절차가 미국 및 캐나다의 CMVP이고, 실제 암호모듈 검증을 위한 국제기준인 ISO/IEC 19790은 FIPS 140-2와 거의 동일하다. 대부분의 국가가 CMVP를 사용하여 암호모듈을 검증하고 있다. [표 2]는 각 국가별로 CMVP 기준을 분류하고 있다.

[표 2] 각국의 CMVP 기준의 분류

기준별 / 국가별	암호모듈 검증기준 (CMVP)			암호모듈 시험기준 (DTR)		
	기준년	발행년도	상태	기준년	발행년도	상태
미국 및 캐나다 (CMVP)	NIST FIPS 140-1	1994.1	폐지	DTR for FIPS 140-1	1995.3	폐지
	NIST FIPS 140-2	2001.5	현재 표준	DTR for FIPS 140-2	2004.3	현재 표준
	NIST FIPS 140-3	2007.7	초안 (2009.11 개정초안)	DTR for FIPS 140-3	N/A	N/A
국제	ISO/IEC 19790	2006.3	현재 표준	ISO/IEC 24759	2007.5	현재 표준
한국 (KCMVP)	암호검증기준 (FIPS 140-2 참조)	2006.11	현재 표준	암호시험기준 (DTR 참조)	2007.3	현재 표준
	KS X ISO/IEC 19790	2007.12	현재 표준	KS X ISO/IEC 24759	2007.12	현재 표준
일본 (JCMVP)	JIS X 19790 (FIPS 140-2 참조)	2007.3	현재 표준	JIS X 5091 (DTR 참조)	2007.3	현재 표준

3. 암호모듈 평가 및 암호 알고리즘 구현 적합성 평가 기술

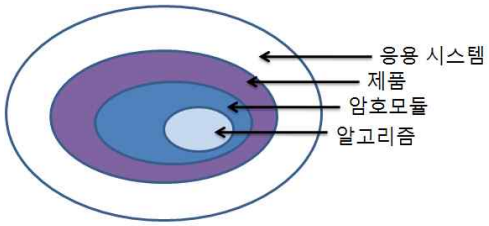
CMVP에서 요구하는 암호 모듈의 안전성 평가는 크게 3가지로 구분할 수 있다.

첫째로 구현 적합성 평가이다. 이 평가는 구현된 암호 기술이 표준에 따라 제대로 구현되었는지를 평가하며, 이는 각 표준에 따라 평가하는 방법이 다름을 의미한다.

둘째로 암호 키 운용 및 관리 평가이다. 이 평가는 암호 기술의 안전성에 직접적인 영향을 미치는 암호키의 생성, 확립, 분배, 입/출력, 저장, 파기 등에 대한 방법 및 과정을 평가함으로서 잘못된 암호 키 운용 및 관리에 따른 암호 키의 유출 가능성을 평가함으로 암호 모듈 안전성 평가에 있어서 가장 중요한 부분이라고 할 수 있다.

셋째로 물리적 보안 평가이다. 이 평가는 암호 모듈의 사용 환경에 대한 평가로 암호 모듈의 운영 환경, EMI/EMC, Self-Testing등에 대한 평가를 의미한다.

가장 기본적이고 중요한 암호 알고리즘에 대한 구현 적합성 평가는 구현된 암호 기술이 표준에 따라 제대로 구현되었는지를 평가하며, 이는 각 표준에 따라 평가하는 방법이 다르다.



Level	평가 기반
응용 시스템	
제품	Common Criteria
암호모듈	FIPS 140-3
알고리즘	FIPS 197

[그림 2] 암호모듈과 평가기반의 관계

위의 [그림 2]에서 같이 CMVP내에서 수행하는 평가의 범위는 정보 보호 제품에서 가장 근간이 되는 암호 알고리즘을 기반으로 한 암호 모듈의 평가에 있다고 할 수 있다.

[표 3] NIST FIPS 승인 알고리즘

구분	표준 번호	제목
대칭키	FIPS PUB 46-3	Triple-DES
	FIPS PUB 185	SkipJack
	FIPS PUB 197	AES
	FIPS PUB 81	DES mode of operation
공개키	FIPS PUB 186-2	DSS
	ANSI X9.31	rDSA
	ANSI X9.62	ECDSA
해쉬함수	FIPS PUB 180-1	Secure Hash Standard
MAC	ANSI X9.19	Enhanced Security DES MAC
	FIPS PUB 113	DES MAC and Triple-DES MAC
keyed Hash	FIPS 198	The keyed-HASH MAC
RNG	FIPS PUB 186-2	DSS Appendix 3.1-2
	ANSI X9.31	rDSS Appendix A
	ANSI X9.62	ECDSA A.4

위의 [표 3]은 FIPS 승인 알고리즘을 표로 간략히 나타낸 것이다. CMVP는 FIPS 승인 표준 알고리즘을 기반으로 블록암호 알고리즘, 공개키 암호 알고리즘, 메시지 인증 코드, 난수 생성, 키관리 등에 대한 구현 적합성 검증방식을 표준화 시키고 이에 대한 구현 적합성 검증을 수행하고 있다.

4. 결론

본 논문에서는 현재 북미에서 활발히 진행 중에 있는 암호 모듈 평가 프로그램인 CMVP에 대한 평가/승인 체계와 기술 사항을 분석하였고 , FIPS 140-x의 표준화와 시험 평가에 대해 연구하였다.

선진각국의 경우에 미국은 자국의 FIPS 표준을 ISO 표준화에 총력을 기울여 FIPS 140-2 가 19170으로, DTR 을 ISO 24759 로 국제표준화 시키고 있다. 캐나다의 경우에는 미국과 초창기부터 공동으로 CMVP를 진행하여 왔으며, 영국의 경우에는 CESG 를 통하여 표준화에 동참하면서도 별도의 CAPS 제도를 운영하고 있다. 일본은 미국의 CMVP를 JCMVP 로 따라서 움직이며, 2개의 평가기관을 발 빠르게 발족하여 표준화에 동참하고 있다.

이제 CMVP는 미국만의 것이 아니라, ISO 표준화로 책정되어 CC 평가와 함께 곧 세계적인 정보보호 제품 평가체계를 구축하게 되었다.

이를 위하여, 미국 및 일본 등의 경우와 같이 조달청 구매 물품 내에 암호모듈인증 제품이 현실적으로 사용될 수 있도록 정부 통합 조직을 구성, 운영되어야 할 것이며, 이를 뒷받침할 수법과 제도가 수립되어야 하며, 사용자, 개발자, 평가자에 대한 기준 및 기술 가이드라인이 정립되어야 한다.

참고문헌

[1] KISA, 공통평가기준 1부, 2부, 3부, 1999.8
[2] 한국 정보보호 진흥원, 암호제품 평가 체계 분석, 2002
[3] 박성근 외 5명, CMVP 테스트를 적용한 SEED 암호 알고리즘 모듈 구현, 2003.05
[4] NIST, Cryptographic Module Validation Program Conference, 2002.03
[5] NIST, Security Requirements for Cryptographic Modules(FIPS 140-2), 2001
[6] NIST, Security Requirements for Cryptographic Modules(FIPS 140-3 Revised DRAFT), 2009
[7] NIST, Cryptographic Module Validation Program(CMVP), http://csrc.nist.gov/cryptval
[8] 한국 정보보호 진흥원, http://www.kisa.or.kr
[9] Lee, Annabelle, Guideline for Implementing Cryptography in the Federal Government, Special Publication 800-21, Gaithersburg, MD, National Institute of Standards and Technology, November, 1999.
[10] 일본 JCMVP : http://www.ipa.go.jp/security/jcmvp
[11] 영국 CESG : http://www.cesg.gov.uk